Viewpoint Paper ■

EHR Safety: The Way Forward to Safe and Effective Systems

JAMES M. WALKER, MD, PASCALE CARAYON, PHD, NANCY LEVESON, PHD,
RONALD A. PAULUS, MD, MBA, JOHN TOOKER, MD, MBA, HOMER CHIN, MD, ALBERT BOTHE, JR., MD,
WALTER F. STEWART, PHD, MPH

Abstract Diverse stakeholders—clinicians, researchers, business leaders, policy makers, and the public—have good reason to believe that the effective use of electronic health care records (EHRs) is essential to meaningful advances in health care quality and patient safety. However, several reports have documented the potential of EHRs to contribute to health care system flaws and patient harm. As organizations (including small hospitals and physician practices) with limited resources for care-process transformation, human-factors engineering, software safety, and project management begin to use EHRs, the chance of EHR-associated harm may increase. The authors propose a coordinated set of steps to advance the practice and theory of safe EHR design, implementation, and continuous improvement. These include setting EHR implementation in the context of health care process improvement, building safety into the specification and design of EHRs, safety testing and reporting, and rapid communication of EHR-related safety flaws and incidents.

■ **J Am Med Inform Assoc.** 2008;15:272–277. DOI 10.1197/jamia.M2618.

Introduction

There is a growing consensus that widespread adoption of electronic health care records (EHRs) is essential to achieving many American health care goals, including improved care quality and patient safety (See Table 1 for definitions). Although the benefits of well-managed EHRs may seem obvious and are likely substantial, the overall safety and effectiveness of EHRs have not been shown.[1,2] Few EHR risk-management strategies have been published.

As is the case with other health care interventions, the safety and effectiveness of EHRs need to be tested and continuously improved. The Committee on Quality of Health Care in America of the Institute of Medicine notes that health care organizations "should expect any new technology to introduce new sources of error and should adopt the custom of automating cautiously, alert to the possibility of unintended harm."[3] Because EHRs are particularly complex technology innovations—affecting workflows, communications, job definitions, working conditions, and job security—demonstrating and improving their safety is critically important.[5–10] This article outlines current knowledge regarding EHR safety and effectiveness and proposes strategies to increase them.

In the first organizations to use EHRs, software designers knew the organization, the EHR's users, and the specific care processes the EHR was meant to support. The decades-long, iterative development process that these early EHRs went through improved the fit between the software and the organization, the users, and the care processes. Because of this extensive customization (a type of overfitting), reports of EHR-related effectiveness from these organizations—although important as efficacy studies—may not be generalizable to the less customized EHRs and EHR implementations that most organizations will use. Later-adopting organizations will range from well-capitalized, integrated health care systems to small, resource-constrained physician practices. The safety and effectiveness of EHRs in these different organizations are likely to vary significantly.[11]

To select, implement, and continuously improve a safe and effective EHR, health care organizations will need well-executed strategies in a number of areas. Those listed in Table 2 are drawn from studies of health care and other industries.[11–15]

Some organizations are executing many of these strategies and may be able to add those they are not. However, as EHR adoption becomes more widespread, organizations with fewer resources will need help to execute many of the strategies—or they will need affordable access to EHRs designed to minimize the need for those strategies.[16]

EHR Safety and Effectiveness

Assessing the overall safety and effectiveness of EHR use is made difficult by the limited research literature. The few available studies have largely been conducted by the developers of the EHRs and have focused on the effect of order

Affiliations of the authors: Geisinger Health System (JMW, RAP, AB), Danville, PA; EHR Safety Institute (JMW), Danville, PA; Department of Industrial and Systems Engineering, and Center for Quality and Productivity Improvement, University of Wisconsin (PC), Madison, WI; Department of Aeronautics and Astronautics, and Department of Engineering Systems and Complex Systems Research Lab, Massachusetts Institute of Technology (NL), Cambridge, MA; American College of Physicians (JT), Philadelphia, PA; Clinical Information Systems, Kaiser Permanente Northwest Region (HC), Portland, OR; Geisinger Center for Health Research (WFS), Danville, PA.

The authors thank Carol Diamond, MD, and Sandra Buckley for their perceptive comments on early drafts of this paper.

Correspondence: James M. Walker, MD, FACP, Geisinger Health System, MC 30-06, 100 North Academy Avenue, Danville, PA 17822-3006; email: <jmwalker@geisinger.edu>.

Received for review: 09/14/07; accepted for publication: 02/13/08.

Table 1 ■ Definitions

Assessors of healthcare or EHR characteristics (including safety and effectiveness): any organization that works to improve healthcare in general or EHRs specifically—for example, Joint Commission, KLAS, CCHIT, Leapfrog, CMMS, and other healthcare payers.

EHR: The system of linked electronic information-management sub-systems used to support direct patient care. The typical EHR is comprised of a growing set of interconnected software applications including but not limited to patient-data repositories with links from feeder systems such as laboratories; electronic communications among clinicians and patients; order management systems (including care planning, order entry, pharmacy order processing, and documentation of medication administration); and data-input devices. Different organizations' EHRs are comprised of unique constellations of information-management subsystems, making a more precise definition misleading. (See Tang, 2003 for a fuller discussion.)[4]

EHR-Related System Flaw: Any characteristic of an EHR or of its interactions with other healthcare systems that has the potential to worsen care quality or patient outcomes. Other healthcare systems include individuals, care teams, facilities, policies, care processes, and healthcare organizations. Flaws may be introduced during the specification, design, configuration, or continuous-improvement phases of the EHR lifecycle.

Safety Incident: a non-routine event which has the potential to contribute to patient harm.

Software Specification (or Software-Requirements Specification): a statement of what a software system should do (See IEEE Standard 830-1998.)

entry (CPOE) systems on a limited number of error types.[17–20] Although some measures of error showed improvement, overall safety and effectiveness have been addressed in only five studies.[21–25] Although the first two studies have been widely cited as showing CPOE benefits, neither showed improvements in patient outcomes.[20–22] In fact, the second study reported an increase in medication errors and adverse drug events, which was reversed after an improvement in the CPOE interface.[22] The third study, conducted in a subpopulation of a children's hospital, documented a doubling of mortality (from 2.8% to 6.6%) after CPOE implementation.[23] The fourth study, conducted in the same hospital, showed no significant change in mortality.[24] The fifth study found that only thirty-one percent of physicians and fifty-six percent of nurses believed that the EHR contributed to improvement of care overall.[25]

In a systematic review of computerized clinical-decision support, Garg et al. concluded that "only seven trials reported improved patient outcomes . . . and no study reported benefits for major outcomes such as mortality. Surrogate patient outcomes, such as blood pressure and glycated hemoglobin, were not meaningfully improved in most studies."[26] A more recent systematic review of health care information technology (largely EHRs) by Chaudhry et al. concluded that in most health care settings, it may be difficult "to determine what benefits to expect from health information technology use and how best to implement the system in order to maximize the value derived."[27] A systematic review of outpatient CPOE systems found only four studies that addressed safety and concluded, "the relatively small number of evaluation studies published to date do not provide adequate evidence that CPOE systems enhance safety and reduce cost in the outpatient settings."[28] Another systematic review of the effect of EHR use on the quality of outpatient care came to a similarly negative conclusion.[29]

Beyond the published literature, what is the evidence that EHRs can support overall improvement in patient safety? One important source of evidence is the experience of organizations that use relatively mature EHRs.[1] In those organizations, including those of the authors, clinicians regard easy access to test results, clinician observations, clinical-decision support, and e-messaging as vital to care quality and patient safety. Patient safety programs, such as medication reconciliation at the transitions between the outpatient and inpatient settings, depend critically on the EHR to make them feasible and effective.

EHR-related Safety Flaws

Complicating matters, the health care literature documents the potential of EHRs to contribute to safety incidents and patient harm.[1,23,30–33] Beyond these published reports, several organizations have collectively identified and documented thousands of potential EHR-related safety flaws.[34] Most of these flaws are identified and mitigated before a safety incident occurs. A small number (anecdotally, <0.1%) are discovered after they contribute to an incident (for example, a medication administration error).

It may well be, as some have argued, that the reports of patient harm say more about the dangers of suboptimal EHR implementation than they do about EHRs per se.[35–37] But to the extent that this is true, it simply raises additional questions: What are the positive and negative effects of EHRs as implemented on care quality, including safety? What implementation factors are associated with those positive and negative effects? What EHR design, implementation, and continuous-improvement practices will lead to maximized positive effects and minimized negative effects? These questions need to be answered as rapidly as possible.

Seven Proposed EHR Safety Steps

In the absence of published research that identifies a comprehensive set of effective risk-reduction activities, health care organizations (large and small), EHR vendors, and EHR assessors need an interim, pragmatic framework for assuring EHR safety. This framework needs to take into account the full EHR lifecycle, including design, implementation in a

Table 2 ■ Organizational Strategies Necessary to EHR Safety

Care-process transformation (thoroughgoing redesign of health care processes to achieve significant improvements in clinical outcomes, service levels, and costs)

Patient safety (consistent, organization-wide efforts to improve care quality and patient outcomes)

Human-factors engineering (fitting technologies to organizational, team, and individual needs)

Software safety (the application of systems engineering methods to reducing the risks associated with software design and use)

Project management (the application of explicit management practices to a project to maximize benefits and minimize costs, including risks)

Continuous improvement (unceasing, systematic efforts to improve processes and outcomes) specific organization, and continuous improvement after implementation. We propose seven steps that health care organizations, EHR vendors, and EHR assessors can undertake in concert to ensure that EHR safety improves even as adoption becomes more widespread.

Use EHRs as Tools for Health Care Process Improvement

Health care organizations should approach EHR implementation and continuous improvement as part of their overall process-improvement efforts. This approach will reinforce the fact that safe and effective use of an EHR requires new organizational policies, processes, work systems, job descriptions, and education.[38,39] This should start with the explicit recognition of safety as a primary goal of all purchasing, implementation, and continuous-improvement efforts. This would require clinical operations leaders, health care informaticians, and systems safety experts to apply their combined theoretical and practical knowledge to each of the stages of the EHR lifecycle. It might include designating an EHR safety officer who reports to the Chief Medical Information Officer or Chief Quality Officer. Smaller hospitals and most physician practices are unlikely to have the resources to mount such an initiative. They will need access to affordable, safe EHRs that require a minimum of local adaptation and testing—what Greenhalgh et. al. refer to as an "augmented product" that includes care-process enhancement recommendations, implementation and continuous improvement services, a help desk, and technical support.[11]

EHR vendors should specify and design their products to support high-performance processes and continuing process redesign. Health care assessors, payers, and policy makers should frame their initiatives and mandates from this same perspective. For example, requiring and paying for improved health care processes and outcomes (that are not feasible without the effective use of an EHR) is likely to be more productive than paying for the implementation of EHRs per se. Finally, researchers should develop theoretical and practical knowledge regarding the safest and most effective ways to use EHRs to support improved care processes. For example, the current narrow focus on order entry (CPOE) should be broadened to address the iterative, interdisciplinary process of order management that physicians, pharmacists, nurses, and others participate in.

Design and Implement Safe EHRs

Health care organizations should understand their EHR-related safety needs and require vendors to address those needs. At its most basic, this means asking what software safety personnel and practices the vendor uses. Larger health care organizations will need to develop consulting relationships or in-house resources in software safety and human factors engineering to guide EHR purchasing, implementation, and continuous improvement.[14,15] Smaller organizations will need access to augmented EHRs and to impartial, actionable information on the safety characteristics of specific products and implementation options.

EHR vendors should make safety a primary goal from the earliest stages of specification and design. Methods developed in other industries will need to be adapted to health care.[14] The Certification Commission for Healthcare Information Technology (CCHIT; http://cchit1.webexone.com) should translate software safety principles and practices into criteria for certification.[14] Leapfrog (http://www.leapfroggroup.org/) and other business coalitions should make good software safety practices a criterion for participation in their programs.

Improve EHRs through Safety Testing and Reporting

As the power of EHRs to influence care decisions is increasingly recognized and EHRs are used to automate increasing numbers of care processes, early recommendations for voluntary, local oversight of EHR safety[40] are likely to be replaced by requirements (perhaps enforced by the U.S. Food and Drug Administration) that EHR vendors and health care organizations test and report publicly on the safety of their software systems. In advance of this, health care organizations should evaluate the safety of their EHRs carefully and document their safety procedures, analyses, and results. Vendors should describe their safety testing programs and any safety flaws they (or one of their customers) discover to all of their customers. Leapfrog has taken an important preparatory step by developing a system for testing the safety and effectiveness of implemented order entry systems.[41]

In this context, it is crucial to remember that testing is only one part (and perhaps the least effective part) of a software safety program. Software safety involves identifying potential system flaws to be controlled and planning how to control them as the system is being specified and design begins. Changing a software system as complex as an EHR after it has been developed (or implemented) is enormously difficult, error-prone, and expensive. For this reason—and even more importantly for patient safety—proactive safety efforts must be emphasized over reactions to safety flaws or incidents discovered in the field.[14]

A consulting company, KLAS (http://www.healthcomputing.com/Klas/Site/), surveys hundreds of health care organizations on their experiences with specific software products every year. Organizations conducting EHR safety surveys, such as KLAS, should add questions such as these to their survey: "Does the vendor notify you proactively of EHR-related safety flaws and recommend risk-mitigation strategies?" and "Does the vendor respond promptly when you identify a potential EHR-related safety flaw?" Finally, researchers should study how EHRs can be tested in ways that are both informative and resource efficient.

Prevent and Manage EHR-related Incidents

Local EHR implementation and continuous-improvement teams make many decisions—regarding organizational policies, work processes, and software configurations—that have the potential to create system-safety flaws. If it identifies a potential flaw, an organization should notify its EHR vendor, who may be able to provide a software enhancement that removes the flaw. If the flaw cannot be removed by changing the software, the organization may need to change a process or policy. If this is not possible, the organization should remove the function from the EHR. If that is not feasible, users must be warned during training (and in some cases repeatedly after go-live). Organizations should track their efforts to mitigate each flaw and any safety incidents that occur.

The identification of EHR-related flaws increases markedly with every new software deployment (both original implementations and upgrades).[22,42] This makes ample numbers of "shadow trainers" (who observe EHR users, answer questions, provide just-in-time education, and report flaws to the command center) a necessity.[11] A 24-hour command center that scans for flaws and incidents, makes rapid fixes, and communicates them to users is also essential. This support team should distill lessons learned into new (or refined) procedures for future software design, configuration, testing, and training.[13]

A second rapid-response team is needed to manage EHR-related safety incidents. This team should include leaders of clinical operations, the EHR support team, informatics, information security, patient safety, risk management, and public relations. The team must be capable of meeting on a few hours' notice to plan and carry out corrective action. All EHR users who might encounter the flaw that led to the incident must be warned of the flaw while the rapid-response team simultaneously ensures that the flaw is removed from the system and plans any necessary patient communications and other remedial actions. Smaller organizations will need to scale their rapid-response team to the available resources. This need will provide another incentive for smaller organizations to subscribe to an augmented EHR product that provides incident-management support or to join an EHR cooperative. Interorganizational patient safety collaboratives should aid organizations large and small by adding EHR safety to their agendas.[43]

Communicate Safety Flaws and Incidents

When significant safety flaws or incidents are identified, multiple EHR stakeholders need rapid notification. Professional societies (such as the Association of Medical Directors of Information Systems) and EHR users' groups have recently begun using e-mail list-serves as informal notification systems. Vendors are also beginning to notify their customers of flaws (along with solutions). To make these systems maximally effective, organizations that use EHRs should notify their vendors promptly of the flaws they identify. Some of these flaws will turn out to be related to the vendor's software creation process; others will have been introduced by the customer or by interactions between the EHR and other health care systems. Often, this distinction will be difficult to make. In any case, vendors should search for other instances of the flaw and recommend to their other customers appropriate software upgrades or configuration changes. (Even when flaws are created by local configurations or interactions between local EHRs and other systems, the vendor will often be able to create the most effective solution by redesigning the EHR software across its different modules, for example, inpatient, outpatient, and pharmacy in the case of medication reconciliation.)

EHR users and vendors should also submit the flaws and incidents they identify to a national clearinghouse. This clearinghouse should be managed by a trusted organization and designed so that each organization can review the data it submits as well as viewing all the data from its vendors' customers and the entire clearinghouse in anonymized form. Vendors should be able to see the data submitted by their customers as well as the whole database—both in anonymized form. Researchers should have access to the complete, anonymized database. This database would provide all of these stakeholders critical information on the full range of EHR-related flaws and incidents and their frequencies of occurrence. Payers, regulators, and policymakers will need to explore methods for protecting participants' confidentiality and providing incentives for participation.

The clearinghouse should be based on a well-designed taxonomy of EHR-related system safety flaws and safety incidents, which has yet to be developed. Published reports of CPOE-related errors have provided initial, high-level typologies of safety incidents.[30,44,45] However, their focus on order entry is a substantial limitation, because flaws and incidents are not limited to the order entry phase of care.[46] Indeed, where multiple EHR components are integrated (for example, order entry, nursing and pharmacy order processing, and medication administration documentation), one of the most important sources of EHR-related flaws is the interactions among the components.[15] In addition, the published typologies have not addressed such critical issues as the effect of the level of clinical-decision-support automation on safety flaws and their likelihood of contributing to a safety incident.[14,47]

Develop and Communicate EHR Safety Best Practices

Health care organizations should document their policies and procedures (including testing and flaw tracking) for ensuring EHR safety and review them annually. Assessors such as the Joint Commission should monitor compliance. EHR vendors should include EHR safety best practices in their implementation training and documentation. Users' group meetings should provide information on evolving EHR safety best practices.

An important next step in improving EHR safety will be to convene experts from clinical practice, clinical operations, informatics, human factors engineering, information technology, and patient safety to create consensus on what is currently known about assuring EHR safety. Human factors engineers and educators should then lead the development of usable tools that enable health care organizations and EHR vendors to follow those best practices routinely. Finally, systematic research into the prediction, prevention, and management of EHR-related safety flaws and incidents is needed to create the knowledge base on which improved health care processes and EHRs can be built.

Conclusions

Knowledge of how to develop, implement, and continuously improve EHRs for patient safety is currently limited and not accessible to most health care organizations. Health care organizations, EHR vendors and assessors, health care informaticians, safety engineers, human factors engineers, and other stakeholders must organize and disseminate what is currently known and create a reporting system that will advance understanding of EHR-related safety flaws. They must work together to advance EHR safety knowledge and practices so that no patient is harmed by an EHR.

References ▪

1. McDonald C. Computerization can create safety hazards. Ann Int Med 2006;144:510–16.
2. Brown M, Grimm N, Shaw N. The relationship between electronic health records and patient safety: a joint report on future directions for Canada. Toronto, ON: Canada Health Infoway, 2007, pp 1–31.
3. Kohn L, Corrigan J, Donaldson M, To Err Is Human: Building a Safer Health System. Washington, DC: National Academy Press, 1999.
4. Tang P. Safety CoDSfP. Key Capabilities of an EHR System. Institute of Medicine, 2003, p 19.
5. Carayon P, Karsh B. Sociotechnical issues in the implementation of imaging technology. Behav Inform Technol 2000;19:247–62.
6. Eason K. Understanding the organizational ramifications of implementing information technology systems. In: Helander M, Landauer T, Prabhu P, editors. Handbook of Human-Computer Interaction. New York, NY: Elsevier Science, 1997, pp 1475–95.
7. Eason K. Changing perspectives on the organizational consequences of information technology. Behav Inform Technol 2001;20: 323–8.
8. Karsh B. An examination of employee participation during new technology implementation. In: Human Factors and Ergonomics Society 41st Annual Meeting Proceedings, 1997, pp 767–71.
9. Nolan T. Understanding medical systems. Ann Intern Med 1998;128:293–8.
10. Smith M, Carayon P. New technology, automation, and work organizations: stress problems and improved technology implementation strategies. Int J Human Factors Manuf 1995;5:99–116.
11. Greenhalgh T, Robert G, Macfarlane F, Bate P, Kyriakidou O. Diffusion of innovations in service organizations: systematic review and recommendations. Millbank Q 2004;82:581–629.
12. Ash JS, Stavri PZ, Kuperman GJ. A consensus statement on considerations for a successful CPOE implementation. J Am Med Inform Assoc 2003;10:229–34.
13. Walker JM, Richards F, Bieber E, editors. Implementing an Electronic Health Record System. New York: Springer, 2005.
14. Leveson N. Safeware: System Safety and Computers. Reading, MA: Addison-Wesley, 1995.
15. Kleiner B. Sociotechnical System Design in Health Care. In: Carayon P, editor. Handbook of Human Factors and Ergonomics in Health Care and Patient Safety. Mahwah, NJ: Lawrence Erlbaum, 2007.
16. Lehmann C, Kim G. Computerized Provider Order Entry and Patient Safety. Pediatr Clin North Am 2006;53:1169–84.
17. Kaushal R, Bates D. Computerized physician order entry (CPOE with clinical decision support systems [CDSSs]). In: Wachter R, editor. Making Health Care Safer: A Critical Analysis of Patient Safety Practices. Evidence Report/Technology Assessment No. 43. Rockville, MD: Agency for Healthcare Research and Quality, 2001.
18. Kaushal R, Shojania K, Bates D. Effects of computerized physician order entry and clinical decision support systems on medication safety; a systematic review. Arch Intern Med 2003; 163:1409–16.
19. Oren E, Shaffer E, Guglielmo B. Impact of emerging technologies on medication errors and adverse drug events. Am J Health Syst Pharm 2003;60:1447–58.
20. Berger R, Kichak J. Computerized physician order entry: helpful or harmful? J Am Med Inform Assoc 2004;11:100–3.
21. Bates DW, Leape LL, Cullen DJ, et al. Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. JAMA 1998;280:1311–6.
22. Bates DW, Teich JM, Lee J, et al. The impact of computerized physician order entry on medication error prevention. J Am Med Inform Assoc 1999;6:313–21.
23. Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold CPOE system. Pediatrics 2005;116:1506–12.
24. Del-Beccaro M, Jeffries H, Eisenberg M. Computerized provider order entry implementation: no association with increased mortality rates in an intensive care unit. Pediatrics 2006;118: 290–5.
25. Weiner M, Gress T, Thiemann DR, et al. Contrasting views of physicians and nurses about an inpatient computer-based provider order-entry system. J Am Med Inform Assoc 1999; 6:234.
26. Garg AX, Adhikari NKJ, McDonald H, et al. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes. JAMA 2005;293:1223–38.
27. Chaudhry B, Wang J, Wu S, et al. Impact of HIT on quality, efficiency, and costs of medical care. Ann Int Med 2006;144:E-12–22.
28. Eslami S, Abu-Hanna A, deKeizer N. Evaluation of outpatient computerized physician medication order entry systems: a systematic review. J Am Med Inform Assoc 2007;14:400–6.
29. Linder JA, Ma J, Bates DW, Middleton B, Stafford RS. Electronic health record use and the quality of ambulatory care in the United States. Arch Intern Med 2007;167:1400–5.
30. McNutt R, Abrams R, Aron D. Patient safety efforts should focus on medical errors. JAMA 2002;287:1997–2001.
31. Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA 2005;293:1197–203.
32. Nebeker JR, Hoffman JM, Weir CR, Bennett CL, Hurdle JF. High rates of adverse drug events in a highly computerized hospital. Arch Intern Med 2005;165:1111–6.
33. Horsky J, Kaufman DR, Oppenheim MI, Patel VL. A framework for analyzing the cognitive complexity of computer-assisted clinical ordering. J Biomed Inform 2003;36:4–22.
34. Campbell E, Sittig D. Types of unintended consequences related to computerized provider order entry. J Am Med Inform Assoc 2006;13:547–56.
35. Longhurst C, Sharek P, Hahn J, Sullivan J, Classen D. Perceived increase in mortality after process and policy changes implemented with computerized physician order entry. Pediatrics 2006;117:1450–1.
36. Rosenbloom S, Harrell F, Lehmann C, Schneider J, Spooner S, Johnson K. Perceived increase in mortality after process and policy changes implemented with computerized physician order entry. Pediatrics 2006;117:1452–5.
37. Sittig D, Ash J, Zhang J, Osheroff J, Shabot M. Lessons from "Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system". Pediatrics 2006;118:797–801.
38. Carayon P, Hundt AS, Karsh B-T, et al. Work system design for patient safety: the SEIPS model. Qual Saf Health Care 2006; 15(Suppl 1):50–8.
39. Karsh B-T. Beyond usability: designing effective technology implementation systems to promote patient safety. Qual Saf Health Care 2004;13:388–94.
40. Miller RA, Gardner RM. Summary recommendations for responsible monitoring and regulation of clinical software systems. Ann Intern Med 1997;127:842.
41. Kilbridge P, Welebob E, Classen D. Development of the Leapfrog methodology for evaluating hospital implemented inpatient computerized physician order entry systems. Qual Saf Health Care 2006;15:81–4.
42. Shulman R, Singer M, Goldstone J, Bellingan G. Medication errors: a prospective cohort study of hand-written and computerised physician order entry in the intensive care unit. Crit Care 2005;9:R516–21.

43. Carayon P, Kosseff A, Borgsdorf A, Jacobsen K. Collaborative initiatives for patient safety. In: Carayon P, editor. Handbook of Human Factors and Ergonomics in Health Care and Patient Safety. Hillsdale, NJ: Lawrence Erlbaum, 2007.

44. Ash JS, Sittig DF, Dykstrab RH, Guapponea K, Carpenterc JD, Seshadria V. Categorizing the unintended sociotechnical consequences of CPOE. J Med Inform 2007;76:S21–S27.

45. Ash J, Sittig D, Poon E, Guappone K, Campbell E, Dykstra R. The extent and importance of unintended consequences related to computerized provider order entry. J Am Med Inform Assoc 2007;14:415–23.

46. Fortescue EB, Kaushal R, Landrigan CP, et al. Prioritizing strategies for preventing medication errors and adverse drug events in pediatric inpatients. Pediatrics 2003;111: 722–9.

47. Parasuraman R, Sheridan TB, Wickens CD. A model for types and levels of human interaction with automation. IEEE Trans Syst Man Cybern A Syst Humans 2000;30:286–97.